D1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **02-252027**

(43)Date of publication of application : **09.10.1990**

(51)Int.Cl. **G06F 11/10**

G09C 1/00

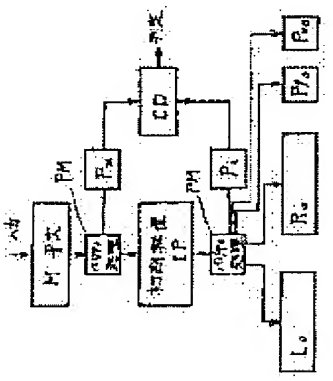
(21)Application number : **01-071974**

(22)Date of filing : **27.03.1989**

(71)Applicant : **HITACHI SHONAN DENSHI CO LTD**

(72)Inventor : **SHIRAISHI TAKAYOSHI**

(54) ERROR DETECTING METHOD



(57)Abstract:

PURPOSE: To detect an error even at the time of ciphering by executing parity check by utilizing a phenomenon changing only the arrangement of parity bits without changing them at the time of inverting processing or the like.

CONSTITUTION: A plane sentence in a plane sentence buffer M is processed by a parity check processing part PM to form a parity and the parity is stored in a parity check bit register Pm. On the other hand, the plane sentence is inverted and ciphered by an initial inverting part IP and the parity of the ciphered sentence is formed by the other parity processing part PM and stored in a parity check bit register Pi. The contents of the registers Pm, Pi are compared with each other by a parity bit comparing part CD and an error in the inverted cipher sentence is detected by utilizing the phenomenon only the array of the parity bits is changed by the inversion without changing the parity bits themselves. Error detection in ciphering processing based upon character conversion or exclusive OR operation is similarly executed to detect an error in a ciphering device.

Detailed Description of the Invention:

.....

Hereinafter, an embodiment of the present invention will be explained in accordance with a cryptographic processing flow of Data Encryption Standard (DES) shown in Figure 1.

First, an error detection method in each portion of a cipher device will be explained.

A plain text to be encrypted is inputted in a plain text register M. Here, a parity check bit P_M is added.

A first process of encrypting is executed in an initial transposition portion (IP) to obtain a parity bit P_i of output, and it is confirmed whether or not $P_M=P_i$ ... (1).

When this is explained in an embodiment of Figure 2, the plain text inputted in a plain text buffer M executes a parity bit calculation by a parity processing portion PM_M during transmission to the initial transposition portion IP, and the obtained result is inputted in a parity check bit register P_M. An output of the initial transposition portion IP is inputted in the parity check processing portion PM. The obtained result is inputted in a parity check bit register P_i. At this time, a parity of the data in a left register L_0 is inputted in a parity check bit register Pl_0, and a parity bit of the data in a right register R_0 is inputted in a parity check bit register P_R.

Error determination is executed by a parity bit comparison portion CD by obtaining output from parity registers P_M and P_i, the obtained result outputs a determination signal (no error is "0" and existence of an error is "1").

A basic algorithm of the above-described DES is an exclusive OR⊕ of a cryptographic function portion f and a left register L with 16-time repetition as shown in Figure 1. Error detection relating to this will be explained in an embodiment of Figure 3.

.....

Figure 1

(a) CRYPTOGRAPHIC PROCESSING PORTION

#1 M PLAIN TEXT (64)

#2 INITIAL TRANSPOSITION IP

#3 THE FIRST STAGE

#4 THE 16TH STAGE

#5 FINAL TRANSPOSITION IF^{-1}

#6 ENCRYPTED TEXT (64)

(b) KEY PRODUCING PORTION

#7 K KEY (64)

#8 REDUCED TRANSPOSITION PC-1

#9 KL KEY (56)

#10 LEFT SHIFT

#11 REDUCED TRANSPOSITION PC-2

#12 THE NUMBER OF BITS IN PARENTHESES

IP: INITIAL TRANSPOSITION PORTION
L: LEFT REGISTER
R: RIGHT REGISTER
f: CRYPTOGRAPHIC FUNCTION PORTION
IF^{-1}: FINAL TRANSPOSITION PORTION
PC-1: KEY INITIAL REDUCED TRANSPOSITION PORTION
PC-2: KEY REDUCED TRANSPOSITION PORTION
M: PLAIN TEXT REGISTER
K: KEY REGISTER
C: CIPHER REGISTER